

IC, IC-MOUNTED ELECTRONIC DEVICE, DEBUGGING METHOD AND
IC DEBUGGER

BACKGROUND OF THE INVENTION

5

1. Field of the Invention

The present invention relates to an IC, an electronic device, a method for debugging the IC, a method for debugging the electronic device, and a debugger, having a security function for preventing a spurious acquisition of a behavior of an internal circuit of the IC.

2. Description of the Related Arts

In every field such as an electronic commerce, etc., a device of higher security is demanded. For this reason, various methods for preventing a reverse engineering in the device are devised. However, irrespective of these trials, a reverse engineering ROM, or the like is prepared, and an abuse for a reluctant use for a developer of the device does not become extinct. For this reason, a system in which a third person is incapable of engineering operation itself of the device is demanded.

Fig. 9 is an explanatory diagram of the prior art. As shown in Fig. 9, an LSI 110 is provided with a CPU 200, a peripheral circuit 300, and a bus 600 for connecting therewith. In this LSI 110, the CPU 200 acquires data or programs from the peripheral circuit 300, and processes the data, and outputs them to the

peripheral circuit 300.

On the other hand, in the case where the device is developed by use of this LSI 110, a processing behavior of the CPU 200 is directly monitored, and the programs or the like are verified.

5 A verification method for monitoring output data of the peripheral circuit 300 is executed, but a behavior of the CPU 200 up to the output cannot be elucidated from the output data.

For this reason, the CPU 200 is provided with a debug I/F (interface) circuit 400 via another bus 500. An external
10 debug controller 100 of the LSI 110 is connected to the debug I/F 400, and supplies a clock CLK, and inputs a signal SIN, and obtains an output SOUT.

This debug I/F circuit 400 is exploited for acquiring a behavior (contents of a program counter, a register, or the
15 like) of the CPU 200 at the time of developing the device, and in the case where the device is shipped to a field, the debug I/F circuit 400 is similarly exploited at the time of the occurrence of a fault, and at the time of diagnosing the device.

20 A security function is not provided in the prior art with respect to an access from the debug I/F 400, as described above.

In the device which does not require a conventional normal security, a debug I/F terminal is seen from outside irrespective
25 of the time of being unused/the time of being used, and is entirely defenseless for the exploitation by the third person. For this reason, in the case of the device shipped to the field,

the third person uses the debug I/F terminal, so that a behavior of a central processing unit (CPU) can accurately and readily be made reverse engineering, and it needs high-performance in security.

5 However, in the case where the conventional device uses the CPU provided with the debug I/F function, a clue of analysis is given to the third person. For example, in the case of a POS register using the CPU with the debug I/F function, a debug unit of the debug I/F is connected to a personal computer, 10 etc., so that even data such as a password, a cryptographic key, or the like can readily be searched.

SUMMARY OF THE INVENTION

It is therefore the object of the present invention to 15 provide an IC, an electronic device, a debug method, and a debugger for restricting a use of a debug I/F and preventing a spurious reverse engineering by a third person.

It is another object of the present invention to provide 20 an IC, an electronic device, a debug method, and a debugger in which an authentication logic is provided between the debug I/F circuit in the LSI and an external terminal, and a restriction is formed in exploiting the debug I/F.

It is yet another object of the present invention to 25 provide an IC, an electronic device, a debug method, and a debugger for preventing the engineering of the authentication logic between the debug I/F circuit in the LSIs and the external terminal.

It is a further object of the present invention to provide an IC, an electronic device, a debug method, and a debugger for detecting the spurious reverse engineering by a third person which restricts the use of the debug I/F.

5 In order to attain the above objects, according to a first aspect of the present invention there is provided an IC comprising an internal circuit; a debug I/F circuit for debugging the internal circuit from externally; and an authentication circuit which is provided between the debug I/F circuit and a debug terminal, and when the debug I/F circuit is activated, transmits a transmission key from the debug terminal to outside, and authenticates from a signal received from the debug terminal and a transmission key, and enables operation of the debug I/F circuit.

15 According to a second aspect of the present invention there is provided an electronic device mounting with an IC, the IC comprising an internal circuit; a debug I/F circuit for debugging the internal circuit from externally; and an authentication circuit which is provided between the debug I/F circuit and the debug terminal, and when the debug I/F circuit is activated, transmits the transmission key from the debug terminal to outside, and collates the signal received from the debug terminal with the transmission key, and enables operation of the debug I/F circuit.

25 According to a third aspect of the present invention there is provided a debugging method comprising the steps of transmitting the transmission key to externally when the debug

I/F circuit is activated; and authenticating the signal received from externally and the transmission key to enable operation of the debug I/F circuit.

According to a fourth aspect of the present invention
5 there is provided a debugger for debugging an IC, the IC comprising an internal circuit; a debug I/F circuit for externally debugging the internal circuit; and an authentication circuit which is provided between the debug I/F circuit and the debug terminal, and when the debug I/F
10 circuit is activated, transmits the transmission key from the debug terminal to outside, and collates the signal received from the debug terminal with the transmission key, and enables operation of the debug I/F circuit, further comprising: the discrimination device which is provided between a debug unit
15 and the debug I/F circuit, and receives the transmission key to encode it by a predetermined key, and transmits the reception signal.

Since an authentication circuit is provided between the debug I/F circuit and the debug terminal, it is possible to
20 protect an internal circuit from a dishonesty as performing reverse engineering a motion of the internal circuit, etc. by exploiting the debug I/F of the third person, and to hold security higher than a conventional device.

Furthermore, since the security is performed by a
25 physical connection and an authentication algorithm by a set of a discrimination device and an IC, the high security is enabled. Furthermore, a spurious engineering by a PC (personal

computer) is difficult.

Furthermore, in the debugging method according to the present invention, the authentication step has a step of canceling a reset signal to the debug I/F circuit for enabling of the operation. In the LSI according to the present invention, the authentication circuit cancels the reset signal to the debug I/F circuit for enabling of the operation. For this reason, even if authenticated, it is possible to realize by cancellation of the existent reset.

Furthermore, in the LSI according to the present invention, the authentication circuit forms an authentication key that is encoded the transmission key by a predetermined key, and compares the reception signal with the authentication key. In the debugging method according to the present invention, the authentication step has a step of forming the authentication key that is encoded the transmission key by the predetermined key, and of collating the reception signal with the authentication key. As encoded, the higher security is possible.

In the LSI according to the present invention, the authentication circuit awaits a time of the operation enabling. In the debugging method according to the present invention, the authentication step has a step of waiting a time of the operation enabling. Before and after judgment of a serial data key, a waiting time is provided after the end of agreement judgment by use of a timer. For this reason, even if the third person inputs any cryptographic key data, it takes much time

to obtain authentication results (reset). This causes to prevent the use of the spurious debug I/F by the third person, and furthermore when retrying several times, it takes enormous time.

5 In the LSI according to the present invention, the authentication circuit forms the transmission key with random numbers, whereby each time serial data (transmission key) to be transmitted are activated, the random numbers are based, so that the serial data are set as transmission and reception
10 data different every time, rendering the analysis thereof difficult.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of an LSI according to an
15 embodiment of the present invention;

Fig. 2 is an explanatory diagram of an authentication processing of Fig. 1;

Fig. 3 is an explanatory diagram of a debugging method of the LSI of Fig. 1;

20 Fig. 4 is an explanatory diagram of preventing a spurious access to the LSI of Fig. 1;

Fig. 5 is an explanatory processing of another authentication processing of Fig. 1;

25 Fig. 6 is an explanatory diagram of an electronic device mounting the LSI of Fig. 1;

Fig. 7 is a block diagram of a peripheral circuit of Fig. 1;

Fig. 8 is a configuration diagram of a POS system mounting the LSI of Fig. 6; and

Fig. 9 is an explanatory diagram of the prior art.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The preferred embodiments of the present invention will now be described by sorting it into a LSI, an electronic device, and other embodiments.

[LSI]

Fig. 1 is a block diagram of an LSI and a debug mechanism according to a first embodiment of the present invention, and Fig. 2 is an explanatory diagram of the authentication processing, and Fig. 3 is a diagram for explaining operation at the time of a due use, and Fig. 4 is a diagram for explaining operation at the time of a spurious use.

In Fig. 1, reference numeral 2 denotes a system LSI with a CPU, and a debug I/F utilization authentication circuit according to the present invention is provided to the LSI 2. Reference numeral 1 denotes an external debug controller for utilizing the debug I/F inside the LSI 2. Reference numeral 3 denotes a discrimination device, which is used by interposing it between the LSI 2 and the debug controller 1, so as to interlock with the authentication circuit inside the LSI 2 and authenticate.

The LSI 2 has a debug I/F circuit 2-1, a CPU 2-2, a debug bus 4-1 for connecting an I/F circuit 2-1 and the CPU 2-2, and a peripheral circuit 2-12 connected to a CPU bus 4-2. The

peripheral circuit 2-12 is different according to the use of LSIs, for example, an electronic money funds transferring circuit that will be explained in Fig. 6 on.

In the embodiment of the present invention, the authentication circuit is provided in this CPU bus 4-2. A structure of the authentication circuit is explained.

A port 4-2 receives write data of the CPU 2-2 from the bus 4-2. A register 2-5 stores a debug I/F utilization transmission key formed by the CPU 2-2. A register 2-8 stores an authentication key formed by the CPU 2-2. A transmission circuit 2-4 transmits the transmission key of the register 2-5 in synchronism with a clock supplied by the discrimination device 3. A shift register 2-6 receives a cryptographic key returned from the discrimination device 2.

An agreement detection circuit 2-9 compares a cryptographic key of the shift register 2-6 with an authentication key of a register 2-8, and detects an agreement. A timer circuit 2-7 starts counting clocks in response to an agreement detection output of the agreement detection circuit 2-9, and forms a signal for canceling a reset signal to the internal debug I/F circuit 2-1 after a constant time. A reset gate 2-11 cancels an input to the debug I/F circuit 2-1 of the reset signal according to a reset cancellation signal. A reception-enabling gate 2-10 enables the shift register 2-6 which fetches in data from a signal input terminal SIN in response to a reception-enabling signal from a transmission circuit 2-4.

Next, the discrimination device 3 is provided with a key reception circuit 3-1. When the discrimination 3 is turned on, the key reception circuit 3-1 transmits clocks and receives the aforesaid transmission key, and encodes it by a key
5 determined previously and transmits the cryptographic key.

Next, an operational procedure capable of utilizing the debug I/F will be explained with reference to Figs. 1 and 2. As shown in Fig. 1, the debug controller 1 utilizing the debug I/F is connected to the LSI 2 via the discrimination device
10 3.

① First, the LSI 2 and discrimination device 3 are turned on and activated. Then, a clock is supplied from the discrimination device 3 to the debug I/F 2-1 of the LSI 2. Concurrently, the CPU 2-2 is activated in the LSI 2, and the
15 LSI 2 forms the debug I/F utilizing transmission key and authentication key by a firmware, and writes them into the registers 2-5, 2-8 via the bus 4-2 and port 2-3. At this time, the transmission key is formed based on a random number, and then the authentication key is generated by encoding the
20 transmission key by a predetermined key.

② When the key is written, the transmission circuit 2-4 transmits the transmission key in synchronism with a clock supplied by the discrimination device 3.

③ The key transmission and reception circuit 3-1 in the
25 discrimination device 3 receives the transmission key, and encodes the transmission key by the key determined previously, and transmits the cryptographic (encoded) key. The

predetermined key at this time is same as the key used a little while ago by the firmware in the LSI 2.

④ In the LSI 2, the shift register 2-6 receives the returned the cryptographic key, and the agreement detection circuit 2-9 compares it with the authentication key of the register 2-8, and only in the case where agreed, the agreement detection circuit 2-9 transmits the agreement detection to the timer circuit 2-7. The timer circuit 2-7 waits for a constant time, and canceled a reset signal to the internal debug I/F 2-1 by the gate 2-11.

Thus, for the first time, the debug I/F circuit 2-1 of the LSI 2 can be utilized. Namely, the reset signal is transmitted from the debug controller 1 to the LSI 2, and resets the debug I/F circuit 2-1, and utilizes the debug I/F circuit 2-1, and can access the CPU 2-2.

As shown in Fig. 3, a LSI provider offers the LSI 2 and discrimination device 3 to a developer for an apparatus. The encryption key of the LSI 2 is same with the encryption key of the discrimination device 3. The developer mounts the LSI 2 on the target board 7, and develops the device.

In the case where the debug is performed, the LSI 2 is connected to the discrimination device 3, which is connected to the debug controller 1, the PC interface board 6, and the personal computer 5. When the discrimination device 3 intervenes therebetween, the above authentication sequence works to cancel a reset, so that the debugger on the PC 5 can utilize the debug I/F circuit 2-1. Furthermore, even after

the device is shipped to a field, the discrimination device 3 is connected, thereby utilizing the debugger on the PC 5.

On the other hand, as shown in Fig. 4, in the case where the discrimination device 3 is not connected, the reset is not canceled in the debug I/F circuit 2-1 of the LSI 2, and the debugger of the PC 5 cannot access the CPU 2-2 of the LSI 2. For example, after the device is shipped to the field, it is possible to protect the CPU 2-2 from dishonesty such as reverse engineering of internal operation of the CPU 2-2 by utilizing the debug I/F of the third person, and to hold the higher security than the conventional device.

Namely, in a security technique such as a conventional password authentication, etc., if the password is leaked, the security function is not performed, and the password is easy to elucidate by retrying. Accordingly, the security technique is unfit as a security mechanism of the LSI 2 to be presented to a great number of users. According to this embodiment, since in order to realize the security with a set of the discrimination device 3 and LSI 2, the security is carried out by the physical connection and authentication algorithm, the high security is enabled. Furthermore, the spurious engineering by the PC 5 is difficult.

Furthermore, in some cases, since the aforesaid utilization authentication function is an encryption algorithm, a skillful spurious person knows existence of the authentication mechanism and tries the engineering by retrying the encryption key (data). According to this embodiment, since

this engineering becomes difficult, the next technique is adopted.

First, after the serial data key is judged, waiting time is provided after end of the agreement judgment by use of the timer 2-7. For this reason, even if the third person inputs any cryptographic key data by connection of Fig. 4, it takes much time until obtaining authentication results (reset). Thus, the spurious debug I/F utilization by the third person is prevented, and it takes enormous time when retrying several times.

Second, each time the serial data (transmission key) to be transmitted are activated, the random numbers are based, so that the engineering becomes difficult as set as transmission and reception data different each time.

Third, the reception operation of the shift register is conducted for a constant time after the transmission key is transmitted, and only one time reception is made at the time of one time activation, and since if data are repeatedly input, not accepted, the engineering is difficult.

Next, in Fig. 5, the authentication processing according to another embodiment of the present invention will be explained.

① First of all, when the LSI 2 and discrimination device 3 are turned on, a clock is supplied from the discrimination device 3 to the debug I/F 2-1 of the LSI 2. Concurrently, in the LSI 2, the CPU 2-2 is activated to form the debug I/F utilization transmission key and authentication key by the

firmware, as described above, to write them into the registers 2-5, 2-8 via the bus 4-2 and the port 2-3.

② When the key is written, in synchronism with the clock supplied by the discrimination device 3, the transmission circuit 2-4 transmits the transmission key.

③ The key transmission and reception circuit 3 in the discrimination device 3 receives the transmission key, and encodes the transmission key by the key determined previously, and transmits the cryptographic (encoded) key. The predetermined key at this time is same with the key used a little while ago by the firmware in the LSI 2. The discrimination 3 annexes a user ID and transmits it to the LSI 2.

④ In the LSI 2, the shift register 2-6 receives the returned cryptographic key, and the agreement detection circuit 2-9 compares it with the authentication key of the register 2-8, and only in the case where agreed, the agreement detection circuit 2-9 transmits the agreement detection to the timer circuit 2-7. After the timer circuit 2-7 waits for a constant time, the timer circuit 2-7 cancels an input of the reset signal to the internal debug I/F 2-1 of the gate 2-11. Furthermore, the user ID is logged. For this reason, if information of the transmission key should be leaked, it is possible to specify which user has leaked, from the logged user IDs.

According to the embodiment of the present invention, the description device 3 adopts a method of encoding the received transmission key and use ID by the key, thereby preventing

that the user ID is readily changed.

[Electronic Devices]

Next, electronic devices mounting the aforesaid system LSI 2 will be explained. Fig. 6 is an explanatory diagram of an example to which the system LSI 2 is applied, and Fig. 7 is a structural diagram of a peripheral circuit of the LSI 2 in this application example, and Fig. 8 is an explanatory diagram of the electronic devices.

As shown in Fig. 6, the system LSI 2 is a card funds transferring LSI, and has a debit card funds transfer function 40, a credit card funds transfer function 41, an electronic money funds transfer function 42, and other service functions 43. For this reason, the LSI 2 is connected to an IC card reader/writer 30, a magnetic card reader 31, and a display and key 32. Furthermore, as occasion arises, the LSI 2 is connected to a receipt printer 33. These funds transfer functions 40 to 43 are realized by execution of the programs of the CPU 2-2 of the LSI 2.

Accordingly, by mounting this LSI 2, a card funds transfer function is imparted to various electronic devices 50 to 57. These electronic devices are, for example, a POS (point of sales) reader/writer 50, an integrated terminal 51, a mobile terminal 52, an ATM (automatic teller machine) 53, an automatic vending machine 54, a PDA (personal digital assistant) 55, a portable telephone 56, and a PC (personal computer) 57.

The peripheral circuit 2-12 of the LSI 2 for the card funds transfer will be explained with reference to Fig. 7.

The peripheral circuit 2-12 has a smart card controller 60, a MS (Magnetic stripe) control circuit 61, a LCD control circuit 62, a matrix KB control circuit 63, a memory controller 64, and serial I/O ports 69 to 72. In Fig. 7, the above LSI 2 indicates a condition of being mounted on the target board 7, and for clarity of description of the LSI 2, only the CPU 2-2 and peripheral circuit 2-12 (60-64, 69-72) are shown. Of course, the LSI 2 includes the debug I/F 2-1 and the authentication circuit.

The smart card controller 60 reads/writes data of the IC card (called a smart card) via the IC card reader/writer 30. The MS control circuit controls the MS (magnetic stripe) reader 31. The LCD control circuit 62 controls a display of the LCD (liquid crystal display) 32-1. The matrix KB control circuit 63 recognizes an input of a ten key 32-2. The memory controller 64 control an input/output into/from various memories (a ROM 65, a SRAM 66, a FLASH 67, a SDRAM 68) on the board 7. The serial ports 69 to 72 are connected to drivers 73 to 75 of the port 7 for inputting and outputting the serial data. These are each connected to the CPU bus 4-2.

Fig. 8 is a system configuration diagram of the electronic device mounting a funds transferring LSI, showing a POS (point of sales) system. The network 35 is connected to a store controller 20 and a plurality of POS terminals 10. The POS terminals 10 are connected to the IC card reader/writer 30. The store controller 20 and the plurality of POS terminals 10 are provided with the above funds transferring LSIs (called

an IFD), which exchanges directly funds transfer data.

An IC card 34-1 for customers is exchanged messages with a POS IC card 34-2 via the IFD 2, and the POS IC card 34-2 is exchanged messages with the IC card 34-2 of the store controller 20 via an IFD 2, a terminal controller 11, a network 35, the terminal controller 11, and the IFD 2.

For example, in the case where the electronic funds transfer is carried out by the IC card, a customer's data of the IC card 34-1 are stored in the POS IC card 34-2 via the IFD 2. Thereafter, the stored data of the POS IC card 34-2 are stored in the IC card 34-2 of the store controller 20 via the IFD 2, the terminal controller 11, the network 35, the terminal controller 11, and the IFD 2.

In this system, as a route of the electronic funds transfer data is closed by the IFD 2, there is no fear that funds transfer data (a password, an accounting number, a balance, and the like) are leaked. Therefore, safety is high.

However, as described above, if accessing the CPU 2-2 by utilizing the debug I/F, it is possible to make a spurious acquisition of funds transfer data (a password, an accounting number, a balance, and the like), so that there is a fear of abusing. Accordingly, an authentication mechanism according to the present invention is, in particular, valid for such uses.

[Other Embodiments]

In addition to the aforesaid embodiments, the following modifications according to the present invention are possible:

(1) According to the aforesaid embodiments, the reset signal is canceled by the authentication, but a gate may be provided at a clock input side of the debug I/F 2-1, so that a clock input is enabled by the authentication.

5 (2) According to the aforesaid embodiments, the waiting time are provided by the timer after the agreement judgment, but the waiting time may be performed for the judgment by the timer before the agreement judgment.

(3) In the case where the disagreement is detected by the
10 agreement judgment, this can be notified to the peripheral circuit. Thus, the peripheral circuit judges as a spurious access, and for example, it is possible to make a disposition such as erasing of data required for the security.

(4) The system LSI is explained for the card funds transfer,
15 but it may be used as the other applications.

(5) The explanation is made as the debug I/F of the CPU, but the present invention can be applied to the debug I/F of the other circuits.

Although the present invention has been described in
20 light of the preferred embodiments thereof, the present invention could be variously modified without departing from the spirit of the present invention, and those modifications are not to be excluded from the scope of the invention.

As set forth hereinabove, according to the present
25 invention, the following effects are presented.

Since the authentication circuit is provided between the debug I/F circuit and the debug terminal, it is possible

to protect the internal circuit from dishonesty such as the reverse engineering, etc. of operation of the internal circuit by utilizing the debug I/F of the third person, and to hold the security higher than the conventional device.

5 Furthermore, since the security is carried out by the physical connection and authentication algorithm with a set of the discrimination device 3 and LSI 2, therefore, the high security is enabled. Furthermore, the spurious engineering by the PC 5 is difficult.

10

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2